KOREAN PATENT ABSTRACT (KR)

PUBLICATION

(51) IPC Code: H04L 12/22
(11) Publication No.: 2001-0105490 (43) Publication Date: November 29, 2001
(21) Application No.: 10-2000-0025007 (22) Application Date: May 10, 2000

(71) Applicant:
Lee Younga
Contents Korea Ltd.
Dae-young building 604, 139 Youngdeongpo-dong 2ka, Youngdeongpo-Gu, Seoul, Korea

(72) Inventor:
HA, JAE HO

(54) Title of the Invention:

Hacker Detection & Tracing System

Abstract:

Provided is a hacker detection and tracing system, which uses the Netbios function of the network to store all of the information on the outside systems that it had previous contacts with. Therefore, even in cases which the outside system is a PPP user whose IP address changes with each contact or in cases which the outside system attempts contact through a third system it is possible to easily detect and trace whether the outside system has ever attempted or actually hacked into the system. In addition, the real time detection of hacking attempts is easily accomplished by the saving of hacking methods and comparison with the contact type and activities of the outside system after connection. When actual hacking occurs swift apprehension of the hacker is easily accomplished by the real-time notification of the hacking occurrence and the providence of information on the hacker system to hacker crackdown organizations. Furthermore since information of all systems that have been used in hacking is registered and shared the hacker detection and tracing system can prevent any hacking attempts.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.		(11) 공개번호	특2001-0105490
H04L 12/22		(43) 공개일자	2001년11월29일
(21) 출원번호	10-2000-0025007		
(22) 출원일자	2000년05월10일		
---	---
(71) 출원인	주식회사 컨텐츠코리아, 이영아
	대한민국
	150-982
	서울 영등포구 영등포동2가 139 대영빌딩 604호
(72) 발명자	하재호
	대한민국
	459-110
	경기도평택시송탄지역지산동1135번지아주1차107-1004
(74) 대리인	조의제
---	---
(77) 심사청구	있음

(54) 출원명 해커감지 및 추적시스템

요약

본 발명의 해커감지 및 추적시스템은 네트웍의 Netbios의 함수를 이용하여 접속한 외부시스템 자체의 모든 정보를 저장하여, 접속한 외부시스템이 접속시마다 IP주소가 바뀌는 PPP사용자이거나 제 3의 시스템을 경유하여 접속하는 경우에도 과거 해킹을 시도했었던 또는 해킹을 하였었던 시스템인지를 용이하게 감지하고 추적할 수 있다. 또한, 해킹관련방법들을 저장하여 실시간으로 접속한 외부시스템의 접속형태 및 접속 후 활동등을 비교·검색하여 실시간으로 해킹시도여부를 탐지하고, 해킹발생시 해킹발생사실과 해당 해커시스템의 정보를 실시간으로 해커 검거기관에 통보함으로써 해커의 신속한 검거가 용이하다. 더욱이, 한번 해킹에 사용되었던 시스템들은 모두 그 정보가 등록되어 공유됨으로서 해킹에 대한 시도를 원천적으로 봉쇄할 수 있는 효과가 있다.

대표도

도1

색인어

해커탐지, 해커추적, Netbios

명세서

도면의 간단한 설명

도 1은 본 발명이 적용된 해커감지 및 추적시스템의 구성도.

도 2는 해커가 해킹을 위해 본 발명이 적용된 시스템에 접속했을 시 대응하는 과정을 나타내는 순서도.

* 도면의 주요부분에 대한 부호의 설명

10 : 네트웍서버 11 : 웹서버

12 : CGI서버 13 : 해커감지서버

14 : 모니터링서버 15 : CGI경고서버

16 : 제 1데이터베이스 17 : 제 2데이터베이스

18 : 제 3데이터베이스

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 해커감시 및 추적시스템에 관한 것으로, 보다 상세하게는 윈도우즈 운영체제기반의 시스템을 이요한 해커가 해킹을 시도하는 경우 이를 감시하고 역 추적할 수 있는 시스템에 관한 것이다.

최근 들어 대학이나 기업체 등의 컴퓨터시스템에 대한 해킹건수가 급증하고 있으며 그 피해의 심각성도 갈수록 높아지고 있다.

해킹의 피해정도도 갈수록 심각해져 스팸메일 발송 또는 서비스거부 등 '보통'수준의 해킹과 불법침입시도 등 '단순'해킹을 넘어서 시스템관리자의 권한을 도용하거나 시스템파괴, 데이터삭제 등 '심각'한 수준의 피해도 늘어나고 있다.

또한, 현재 전세계 개인 컴퓨터들의 대부분은 윈도우즈를 운영체제로 하여 사용되고 있으며, 이러한 윈도우즈를 기반으로 하는 해킹도 많이 증가하고 있으며, 그 피해도 시스템 파괴, 응용프로그램 및 시스템 서비스 거부, 사용자 ID 및 비밀번호 유출·도용, 문서 유출 등 매우 다양하다.

특히, 개인의 ID와 비밀번호를 빼내어 이를 도용하는 경우가 가장 흔하다.

이러한 해킹을 방지하기 위한 방법으로, 패스워드, 사용자인증시스템, 접속자를 필터링하는 방화벽 설치, 해킹 프로그램을 발견할 수 있는 해킹탐지시스템 및 특정 해킹방지프로그램 설치등이 사용되고 있으나 아직 특별한 해결책이 마련되어있지 않은 실정이다.

발명이 이루고자 하는 기술적 과제

그러나, 이러한 해킹방지를 위한 방법들은 단지 해킹을 탐지하고 이를 차단하기 위한 것이다.

또한, 공격자를 추적하는 경우에도 공격자가 고정IP주소를 가지는 경우 공격자의 IP주소를 검색하여 해당 IP주소가 할당된 시스템을 바로 추적할 수 있으나, 전화접속(PPP)과 같이 공격자가 동적IP주소를 사용하는 경우에는 공격자에 대한 적절한 대응이 이루어지는데 많은 어려움이 있다.

따라서, 본 발명의 목적은 해킹에 사용된 시스템에 대한 모든 정보를 입수하고 이를 분류·저장하여 공유함으로써 해당 시스템으로 다시 해킹을 시도할 시 이를 바로 탐지하고 추적할 수 있는 시스템을 제공하는데 있다.

발명의 구성 및 작용

이와 같은 목적을 달성하기 위한 본 발명의 해커탐지 및 추적시스템은 외부시스템들과 네트웍을 통해 연결될 수 있도록 하며, 접속한 외부시스템들의 정보를 추출하여 저장하고, 해커로 판별된 시스템을 실시간으로 추적하는 네트웍서버, 네트웍을 통해 접속한 외부시스템들에게 웹상에서 데이터를 전송하여 주는 웹서버, 상기 네트웍서버를 통해 접속한 시스템의 접속형태와 접속 후 활동을 실시간으로 탐색하는 CGI서버, 상기 CGI서버의 감지결과를 이용해 접속한 외부시스템이 해킹을 시도하는지를 판별하여, 해킹을 시도한 외부시스템의 모든 정보를 기록하는 해커감지서버, 상기 네트웍서버에 접속한 외부시스템이 과거에 해킹에 사용되었던 시스템인지를 실시간으로 검색하고, 해커로 판정된 시스템의 추적을 지시하는 모니터링서버, 해킹의 발생사실 및 해커 시스템에 대한 정보를 실시간으로 해당 기관에 통보하는 CGI경고서버 및 접속한 외부시스템의 시스템정보, 해킹관련방법들 및 해커로 판별된 시스템의 모든 정보를 저장하는 데이터베이스를 포함한다.

이하, 첨부된 도면들을 참조하여 본 발명의 바람직한 실시예를 설명한다.

도 1은 본 발명이 적용된 해커감지 및 추적시스템의 구성도이다.

네트웍서버(10)는 외부시스템과 네트웍을 통해 연결되도록 해주며 네트웍의 Netbios의 함수를 이용하여 접속한 외부시스템의 모든 정보를 추출하여 기록한다.

그리고, 해커로 판별된 시스템과의 접속을 차단하며, 해당 시스템을 실시간으로 추적한다.

웹서버(11)는 네트웍서버(10)를 통해 접속한 복수의 외부 시스템에게 웹상에서 데이터를 전송하여 준다.

CGI서버(12)는 네트웍서버(10)를 통해 접속한 외부 시스템의 접속형태 및 접속 후 활동등을 감지한다.

해커감지서버(13)는 CGI서버의 감지결과와 기 저장된 해킹관련방법들을 비교·검색하여 접속한 외부시스템이 해킹을 하려는 것인지 아닌지를 판별하며, 해킹을 하려는 경우 해당 시스템의 모든 상황을 기록한다.

그러므로 이러한 해킹관련방법은 가능한 모든 해킹방법 및 해킹유형 등을 수집·분석하여 저장해 놓는 것이 바람직하다.

모니터링서버(14)는 네트웍서버(10)에 접속한 외부시스템이 과거에 해킹에 사용된 시스템인지를 검색하고, 해커로 판정된 시스템을 추적하기 위해 네트웍서버(10)에게 해커 추적명령을 내리고, 그 추적상황을 지속적으로 모니터링한다.

CGI경고서버(15)는 해킹의 발생 및 해커 시스템 추적에 의해 알아낸 해커 시스템의 위치 등 관련정보를 해커검거를 위한 기관에 실시간으로 통보하고 이러한 해커에 대한 정보를 공유하기 위해 다른 시스템들에게 전송해준다.

그리고, 데이터베이스(16, 17 및 18)는 네트웍서버(10)로 접속한 외부 시스템에 대한 정보 및 웹서버(11)가 외부 시스템에 제공해 줄 콘텐츠를 저장하는 제 1데이터베이스(16), 접속한 시스템이 해킹을 시도하는지 알기위한 여러가지 해킹관련방법들과 이전에 해킹을 시도했었던 시스템인지를 알기 위한 해커 시스템들의 리스트를 저장하는 제 2데이터베이스(17) 및 접속한 외부시스템이 해킹을 시도하려는 것으로 판별시 해당 시스템의 시스템정보 및 활동정보를 저장하는 제 3데이터베이스(18)를 포함한다.

물론, 이러한 데이터베이스들(16, 17 및 18)은 하나의 데이터베이스로 통합사용될 수 있다.

도 2는 해커가 해킹을 위해 본 발명이 적용된 시스템에 접속했을 시 대응하는 과정을 나타내는 순서도이다.

외부시스템이 네트웍을 통해 본 발명이 적용된 시스템의 네트웍서버(10)에 접속한다(단계 201).

이때, 네트웍서버(10)는 네트웍의 Netbios의 함수를 이용해 접속한 외부시스템의 모든 정보를 읽어들여 이를 제 1데이터베이스(16)에 저장한다.

Netbios는 네트웍 서비스에 접근하기 위한 인터페이스 규정으로 LAN상에서의 Netbios는 자신만의 고유한 이름을 사용한다. 즉, 각각의 단말은 고유한 이름을 가지고 서로간에 통신한다.

윈도우 NT, 윈도우 95 및 98 등 윈도우기반의 컴퓨터들은 고유한 Netbios 이름을 가지고 있어 단순히 IP주소가 아니라 해당 시스템자체의 모든 정보를 추출하여 기록한다.

모니터링서버(14)는 네트웍서버(10)가 읽어들인 정보를 이용해 이를 제 3데이터베이스(18)에 기 등록된 해커시스템들과 비교하여 접속한 시스템이 과거에 해킹에 사용된 시스템인지 아닌지를 검색한다(단계 202).

접속한 외부시스템이 PPP사용자이거나 제 3의 시스템을 경유하여 이전과 다른 IP주소로 접속을 시도하더라도 네트웍서버(10)가 추출하는 정보는 상술한 바와같이 해당 시스템자체의 정보이고 이러한 정보가 등록되어 비교되므로 동일한 시스템을 사용하여 접속을 시도하는 경우 해커시스템들을 용이하게 비교·검색할 수 있다.

이러한 해커시스템에 대한 정보는 해킹을 하였거나 해킹을 시도했었던 모든 시스템들이 등록되며, 새로이 해킹을 시도하거나 해킹하는 모든 시스템들에 대한 정보가 지속적으로 추가되어 업데이트된다.

또한, 이러한 정보는 본 발명이 적용된 다른 시스템들과 상호 주기적으로 교환되어 공유된다.

단계 202의 검색결과 현재 접속한 시스템이 기 등록된 해커시스템들 중 하나이면, 모니터링서버(14)는 네트웍서버(10)에게 해당 시스템의 접속을 차단하고 해당 시스템의 위치를 추적하도록 명령을 전송한다(단계 203).

모니터링서버(14)는 해커시스템의 추적과 동시에 CGI경고서버(15)로 해킹발생을 경찰 등 관계기관에 알리도록 신호를 보낸다.

CGI경고서버(15)는 모니터링서버(14)로부터 신호를 전송받으면, 경찰 등 해커검거를 위한 관계기관에 실시간으로 해킹발생사실 및 해커시스템의 위치 등 관련정보를 전송(단계 204)하여 해당 기관이 해커를 신속하고 용이하게 검거할 수 있도록 한다(단계 205).

단계 202에서, 검색결과 접속한 시스템이 기 등록된 해커시스템에 해당되지 않은 경우, CGI서버(12)는 해당 시스템의 접속형태 및 접속 후 활동(이동경로)을 실시간으로 지속적으로 탐색한다.

해커감지서버(13)는 CGI서버(12)의 탐색결과를 이용해 접속한 외부시스템의 해킹시도여부를 감지·판별한다(단계 206).

이러한 방법으로 제 2데이터베이스(17)에 해킹에 사용되는 모든 해킹방법을 등록해 두고, 외부시스템의 접속방법을 기 제 2데이터베이스(17)에 저장해둔 해킹방법들과 비교하여 기 저장된 해킹방법 중 어느 한 방법으로 접속을 시도하는지 여부를 감지한다. 그러므로 해커들의 해킹방법들을 연구하여 보다 많은 해킹가능방법들을 저장해 두는것이 중요한 요소중 하나이다.

또한, 합법적인 절차 즉, 외부 시스템이 네트웍서버(10)를 통해 웹서버(11)에 접속하여 콘텐츠를 요청하고, 웹서버(11)가 제 1데이터베이스(16)에 저장된 콘텐츠를 네트웍서버(10)를 통해 해당 외부시스템에 전송하여 주는 절차를 거치지 않고 다른 경로로 접속을 시도하는 경우에도 이를 해킹시도로 판단할 수 있다.

접속한 외부시스템이 합법적인 절차(경로)를 거치는 경우에 웹서버(11)는 해당 시스템이 요청한 콘텐츠를 제공하여 정상적인 서비스가 이루어지도록 한다(단계 207).

그러나, 외부시스템이 등록된 해킹방법 중 어느 한 방법을 이용하거나 합법적인 절차를 거치지 않는 경우, 해커감지서버(13)는 해당 외부시스템에 별도의 ID를 생성·부여한 후 제 1데이터베이스(16) 및 제 2데이터베이스(17)에 저장된 해당 시스템의 모든 정보를 제 3데이터베이스(18)에 저장한다(단계 208).

즉, 제 3데이터베이스(18)는 이렇게 해킹에 이용된 시스템들의 정보만을 별도로 저장·관리하게 되며, 이렇게 등록된 정보는 단계 202에서 모니터링서버(14)가 해커시스템을 검색하는데 사용되는 해커시스템 정보가 된다.

더욱이, 이러한 정보는 본 발명이 적용된 시스템들간에 상호 주기적으로 교환되어 공유되므로, 한번 해킹에 사용된 시스템들은 본 발명이 적용된 모든 시스템들의 감시의 대상이된다.

그러므로, 해킹에 사용된 시스템들은 원천적으로 접속이 봉쇄되며 접속시도와 동시에 추적의 대상이 된다.

해킹시스템에 대한 정보가 제 3데이터베이스(18)에 저장됨과 동시에 단계 203에서와 같이 해당 시스템을 추적하게 되며 이후의 과정은 상술된 과정(단계 203 ~ 단계 205)과 같다.

상술된 경우 이외에도, 본 발명이 적용된 시스템은 ID도용에 대해서 능동적인 대응이 가능하다.

즉, 회원에게 ID를 부여해주면서 회원이 주로 사용하는 컴퓨터들에 대한 정보를 미리 등록하여, 접속시 사용된 ID가 기 등록된 회원의 컴퓨터가 사용한 것인지 등록되지 않은 다른 컴퓨터에서 사용된 것인지를 검색하여 ID의 도용여부를 판별할 수 있다.

또는, 시스템 운영자가 각 회원에게 컴퓨터 설치위치, 접속일자 및 접속시간과 같이 회원의 ID가 사용된 컴퓨터들에 대한 정보를 제공해주어 회원이 아닌 다른 사람에 의해 ID가 사용되었는지 여부를 판별한다.

회원의 ID가 도용된 ID로 등록되면, 도용된 ID로 접속하는 시스템이 있을 경우 이를 추적한다.

발명의 효과

상술한 바와같이, 본 발명의 해커감지 및 추적시스템은 접속한 외부시스템 자체의 정보를 추출·저장하므로 해커시스템이 접속시마다 IP주소가 바뀌는 PPP사용자이거나 제 3의 시스템을 경유하여 접속하는 경우에도 과거 해킹을 시도했었던 또는 해킹을 하였었던 시스템인지를 용이하게 감지하고 추적할 수 있다.

또한, 해킹발생시 해킹발생사실과 해당 해커시스템의 정보를 실시간으로 해커 검거기관에 통보함으로써 해커의 신속한 검거가 용이하다.

더욱이, 한번 해킹에 사용되었던 시스템들은 모두 그 정보가 등록되어 공유됨으로서 해킹에 대한 시도를 원천적으로 봉쇄할 수 있는 효과가 있다.

(57) 청구의 범위

청구항 1.

해커감지 및 추적을 위한 시스템에 있어서,

외부시스템들과 네트웍을 통해 연결될 수 있도록 하며, 접속한 외부시스템들의 정보를 추출하여 저장하고, 해커로 판별된 시스템을 실시간으로 추적하는 네트웍서버;

네트웍을 통해 접속한 외부시스템들에게 웹상에서 데이터를 전송하여 주는 웹서버;

상기 네트웍서버를 통해 접속한 시스템의 접속형태와 접속 후 활동을 실시간으로 탐색하는 CGI서버;

상기 CGI서버의 탐색결과를 이용해 접속한 외부시스템이 해킹을 시도하는지를 판별하여, 해킹을 시도한 외부시스템의 모든 정보를 기록하는 해커감지서버;

상기 네트웍서버에 접속한 외부시스템이 과거에 해킹에 사용되었던 시스템인지를 실시간으로 검색하고, 해커로 판정된 시스템의 추적을 지시하는 모니터링서버;

해킹의 발생사실 및 해커 시스템에 대한 정보를 실시간으로 해당 기관에 통보하는 CGI경고서버; 및

접속한 외부시스템의 시스템정보, 해킹관련방법들 및 해커로 판별된 시스템의 모든 정보를 저장하는 데이터베이스를 포함하는 해커감지 및 추적시스템.

청구항 2.

제 1항에 있어서, 상기 네트웍서버는 네트웍의 Netbios의 함수를 이용하여 상기 접속한 외부시스템의 모든 정보를 추출해내는 것을 특징으로 하는 해커감지 및 추적시스템.

청구항 3.

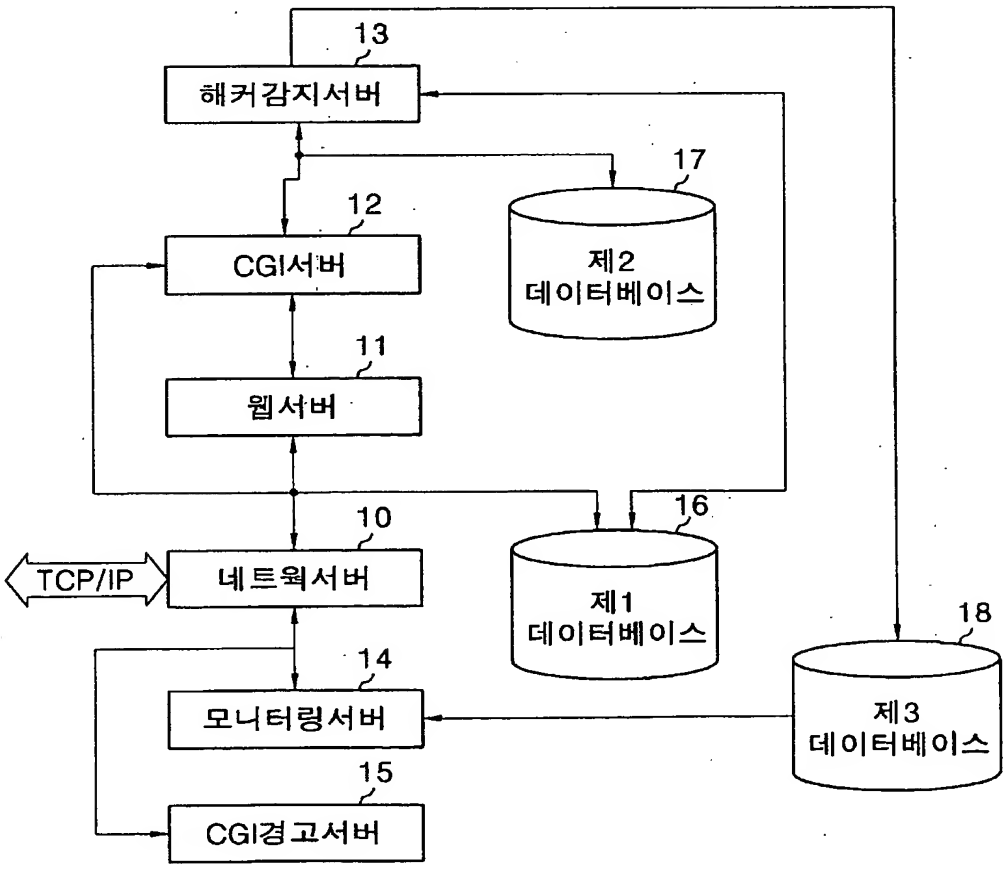
제 1항에 있어서, 상기 해커감지서버는 상기 CGI서버의 감지결과와 기 저장된 해킹관련방법들을 실시간으로 검색·비교하여 해킹의 시도를 판별하는 것을 특징으로 하는 해커감지 및 추적시스템.

청구항 4.

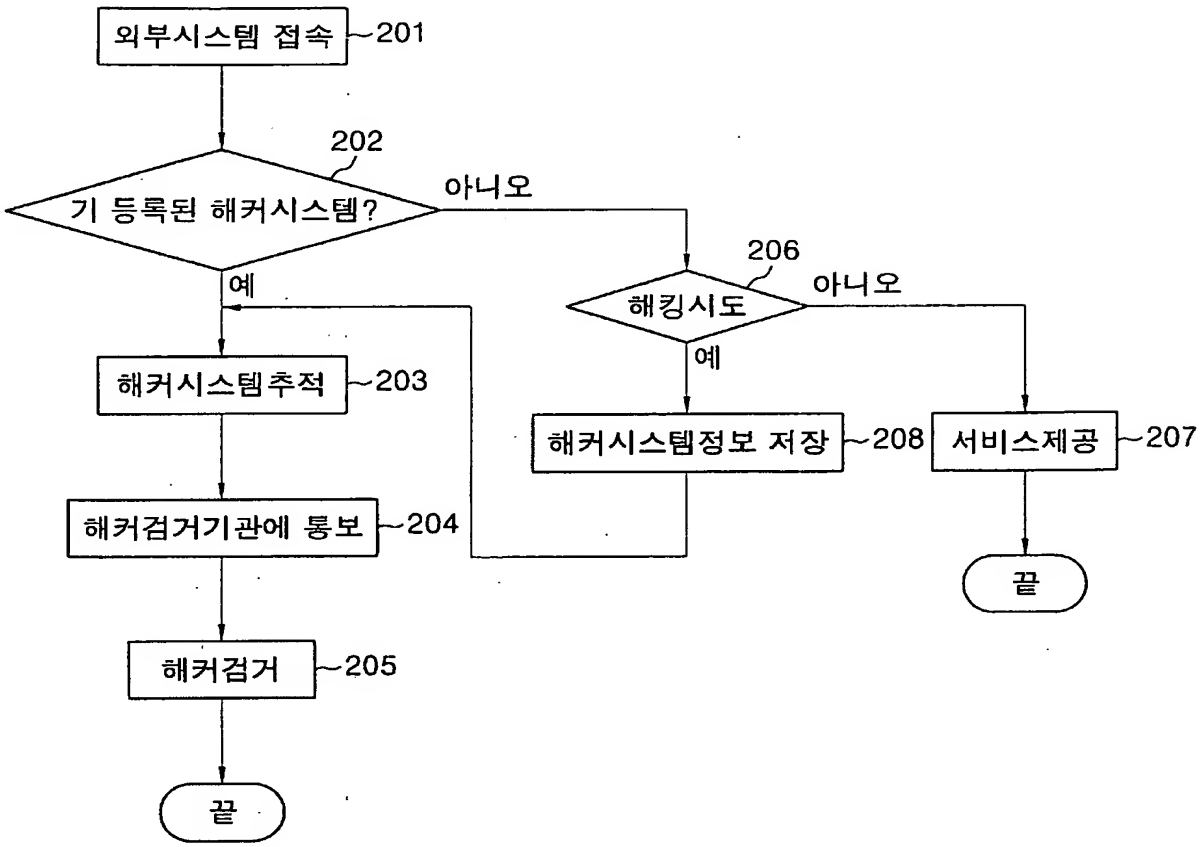
제 1항에 있어서, 상기 해커로 판별된 시스템들에 대한 정보는 타 시스템들간에 상호 주기적으로 교환되어 공유되는 것을 특징으로 하는 해커감지 및 추적시스템.

도면

도면 1



도면 2


외부시스템 접속
201
202
기 등록된 해커시스템?
아니오
예
206
해킹시도
아니오
예
해커시스템추적
203
해커시스템정보 저장
208
서비스제공
207
해커검거기관에 통보
204
끝
해커검거
205
끝